UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/573,684 | 01/04/2007 | Yuichi Futa | 2006_0401A | 3546 |

52349 7590 11/21/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

| EXAMINER | |
|---|---|
| VAUGHAN, MICHAEL R | |
| ART UNIT | PAPER NUMBER |
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/21/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/573,684 | FUTA ET AL. | |
| | Examiner | Art Unit | |
| | MICHAEL R. VAUGHAN | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *21 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,2,5 and 10-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5 and 10-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

The instant application having Application No. 10/573684 filed on 1/4/07 and amended on 10/21/08 is presented for examination by the examiner. Applicant has amended claims 1, 2, 4, 5, and 10-12 and canceled claims 3, 6-9, and 13. Examiner has carefully considered both Applicants' amendments and arguments. Claims 1, 2, 4, 5, and 10-12 are pending.

### *Response to Amendment*

Examiner has reviewed Applicant amendment to the specification and hereby withdraws the aforementioned object to the specification. The amendment also rectifies the previous failings under 35 U.S.C. 101 with regards to unpatentable subject matter. Therefore that rejection is withdrawn. The amendment to claim 4 provides clarity to the scope of the claim and the 35 U.S.C. 112 rejection is withdrawn.

### *Response to Arguments*

Examine has carefully considered Applicants argument with respect to the cited prior art. Examiner respectfully disagrees with the arguments for the following reasons. Applicants have alleged that the prior art of record fails to teach the newly amended limitations in independent claims 1, 2, 11, and 12. Specifically Applicants allege that none of the prior art teaches generating the first encryption key and a first hash key based on the first and second keys. The basis of the argument is centered on the

notion that the encryption key and the hash key are the same key. Whether this is true or not is irrelevant because as the invention is claimed, there is no requirement for the encryption key and hash key to be different. Calling the same entity by two different names does not make the entity different. The claimed invention arrives at a first encryption key and a second encryption which are the same “session key” because of the symmetric encryption process (same key is used for encryption and decryption). The use of the numerals only differentiates which party is using the key. In other words the numerals provide relativity to the key but it is still a common key. Applying the same logic to the newly amended limitations, one can say that the first encryption key is the same hash key. The act of using the key in two different ways gives the key dual meaning. First, the key is used to "encrypt" a message. Next, the key is used to feed a hash module which in the industry is referred to as a hash key. Devadas does in fact teach using the same key for both encryption and hashing. Examiner reiterates that given the language of the claim and the nomenclature used in the claim, there is no requirement for the encryption key and the hash key to be different. Diffie teaches forming an encryption key from two parts. Both sides of the communication arrive at the same encryption key. Devadas teaches using the encryption key also known as the session key in symmetric encryption schemes to feed the MAC module to generate a HMAC (0193-0194). Giving the claim its broadest reasonable interpretable in light of the specification, Examiner finds those limitations obvious in view the prior art of record. Examiner will not, however, import limitations of the specification into the claims. If it is intended for the first encryption key and the first hash key to be different and likewise

the second encryption key and the second hash key, the claims should be amended in such a way to impose those limitations.

As a side note, Examiner would like to point out paragraphs 0044-0046 of Morais, USP Application Publication, previously presented in the prior office action mailed 9/8/08. Even though this prior art was only used in the rejection of claim 4 it has bearing on the aforementioned arguments with regards to the generation of the hash key. Morais teaches two key halves being hashed together to generate a hash key 408. It is known to be a hash key [LAN key] because it is fed into the HMAC module. Morais goes on to teach that this hash key can be used to produce shared secret key. The notion of producing infers that the hash key and the secret key are not the same; rather an operation is performed on the hash key to generate the secret key. In the next paragraph Morais teaches the hash module 410 can generate symmetric keys.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, and 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie in view of USP Application Publication 2003/0204743 to Devadas et al., hereinafter Devadas.

As per claims 1, 2, 11, and 12, Diffie teaches a communication system and method between a first device and a second device, wherein the first device [base] (i) encrypts a 1st key [RN1] using a public key of the second device [mobile] to generate 1st encrypted data, and transmits the 1st encrypted data to the second device (col. 7, lines 50-62)),

(ii) receives 2nd encrypted data from the second device, and decrypts the 2nd encrypted data using a secret key of the first device to obtain a 2nd key [RN2], and (col. 8, lines col. 59-65))

(iii) generates, based on the 1st and 2nd keys, a 1st encryption key [session key] for use in communication with the second device, the second device (col. 8, lines 65-67)

(i) encrypts a 3rd key [RN2] using a public key of the first device to generate the 2nd encrypted data, and transmits the 2nd encrypted data to the first device (col. 8, lines 30-40)),

(ii) receives the 1st encrypted data from the first device, and decrypts the 1st encrypted data using a secret key of the second device to obtain a 4th key [RN1] (Fig. 5a), and

(iii) generates, based on the 3rd and 4th keys, a 2nd encryption key [session key] for use in communication with the first device (col. 8, line 53), and the first and second devices perform encrypted communication using the 1st and 2nd encryption keys (col. 8, lines 48),

wherein the first device generates the first encryption key based on the first and second keys.

Diffie is silent in teaching a first hash key based on the first and second keys, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, and

wherein the second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matched the calculated second hash value. Devadas teaches a first hash key, calculates using the first hash key a first hash value for first transmission data, encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the first hash value and the encrypted first transmission data to the second device, and

wherein the second device generates the second encryption key and a second hash key based on the third and fourth keys, receives from the communication device the first hash value and the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key corresponding to the first

encryption key, calculates using the second hash key a second hash value for the decrypted first transmission data, and determines that the first transmission data is not tampered when the received first hash value matched the calculated second hash value (0193-0194). Diffie uses the two parts of the keys to form a session key whereby data is encrypted. Devadas uses an encryption key or session key as a MAC key [hash key]. The MAC then hashes message with the encryption key to produce an encrypted message with a hash value. Devadas uses this known method of message authentication code to further secure the data packet during transmission. This MAC prevents tampering of the packets. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to use the known method of MAC with the teaching of Diffie because it would increase the security of the system. It is obvious to incorporate other known security measures to strengthen a system.

As per claim 5, the combined system of Diffie and Devadas teaches the key generation unit performs an exclusive OR operation using the 1st and 2nd keys (Diffie, col. 8, lines 47), and generates the encryption key and the hash key based on a result of the operation. Diffie XOR's the key parts to create the session key. Examiner relies on the rationale to combine Devadas and Diffie as disclosed above for using a hash key.

As per claim 10, Diffie teaches the data generation [packet] unit encrypts the 1st key [RN1] based on a key encapsulation mechanism to generate the 1st encrypted key data, and the decryption unit decrypts the 2nd encrypted key data based on a key

decryption mechanism to obtain the 2nd key [RN2] (col. 9, lines 57-63).

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie and Devadas as applied to claim 2 above, and further in view of USP Application Publication 2003/0093669 to Morais et al., hereinafter Morais.

As per claim 4, Diffie and Devadas do not explicitly teach the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value. Morais teaches the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value [0052]. Diffie and Devadas teach using XOR to combine the key parts. Concatenation as taught by Morais of key parts is yet another way to logically combine keys to arrive at another key. This is just a simple substitution of a known function and as such it would have been obvious to one of ordinary skill at the time the invention to substitute another known logical way of combining keys. The combining rationale of Diffie and Devadas is again relied upon to use the newly formed encryption and hash key to generate hash values (MAC).

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed on the enclosed PTO-892 form.

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MRV
2431
/Syed Zia/
Primary Examiner, Art Unit 2431